21337 HOSTETTLER Maël

Attaques par canaux auxiliaires

La sécurité informatique, surtout dans un cadre concret, est un enjeu qui m'a toujours intéressé et qui prend de plus en plus d'importance. En me documentant, j'ai été amené à découvrir le fonctionnement des processeurs et des ordinateurs, ainsi que les différentes manières d'exploiter leurs architectures pour comprendre leur fonctionnement.

L'expansion des villes s'accompagne de l'automatisation de différents services. Ainsi, les enjeux liés à la sécurité informatique de ces services et des flux de données qu'ils engendrent n'en sont que plus grands. De nombreuses applications liées à la modernisation des villes sont potentiellement vulnérables à une attaque par canal auxiliaire.

Positionnement thématique (ÉTAPE 1) :

- INFORMATIQUE (Informatique pratique)
- INFORMATIQUE (Technologies informatiques)

Mots-clés (ÉTAPE 1) :

Mots-clés (en français)	**Mots-clés (en anglais)**
Cryptographie	*Cryptography*
Attaque par canal auxiliaire	*Side channel attack*
Architecture informatique	*Computer architecture*
Mesure de courant électrique	*Electric current measurement*
Corrélation	*Correlation*

Bibliographie commentée

La cryptographie est une technique de protection de l'information : elle vise à protéger une information lors de son acheminement d'un point à un autre. De nos jours, la cryptographie est principalement utilisée pour protéger les systèmes connectés car il est difficile de contrôler physiquement qui tente d'y accéder.

La sécurité des systèmes cryptographiques modernes repose principalement sur la difficulté de résolution de certains problèmes. Certains systèmes cryptographiques ont été « cassés » au sens qu'on peut mathématiquement trouver la clé secrète dans un temps raisonnable. D'autres sont considérés comme sécurisés et des normes comme la norme de sécurité FIPS [5] ont été mises en place pour garantir la sécurité de l'information face à la puissance grandissante des ordinateurs.

Pour autant, même si la sécurité théorique d'un système cryptographique est avérée sous certaines hypothèses (notamment d'informations connues de l'attaquant), ses implémentations réelles ne sont pour autant pas forcément aussi résistantes [1][2]. Ainsi, une attaque par canaux

auxiliaires peut présenter des performances supérieures à une attaque par force brute et impacter les infrastructures réelles et leur sécurité [4].

Les attaques par canaux auxiliaires sont de natures très diverses : par exemple, certaines d' entre elles visent le caractère électromagnétique des composants électroniques en mesurant des consommations de courant électrique ou en captant des émanations électromagnétiques [2][3]. D' autre méthodes moins intrusives que la mesure directe de consommation existent mais requièrent un matériel de pointe ou des informations plus poussées sur la cible (comme l'accès à une région mémoire ou le schéma interne du circuit) : on peut citer par exemple les attaques par mesure acoustique, les attaques par injections de fautes et par analyse du trafic [1][4].

Suite à l'étape de mesure, on obtient des données supplémentaires que l'on peut traiter grâce à des modèles mathématiques pour en déduire des informations confidentielles.

Problématique retenue

On s'interroge sur la faisabilité des attaques par canaux auxiliaires et sur les contre-mesures à mettre en place pour sécuriser les systèmes qui y sont sensibles.

Objectifs du TIPE du candidat

1. Mettre en place une preuve de concept d'attaque par analyse de consommation basée sur une puce Arduino et un oscilloscope analog discovery.

2. Mesurer la consommation de la puce Arduino lors du chiffrement dans le cadre d'un schéma RSA pour en déduire la clé privée.

3. Tenter dans la mesure du possible de réaliser une attaque plus complexe par corrélation visant des systèmes cryptographiques symétriques tels que DES ou AES.

4. Explorer les contre-mesures que l'on peut mettre en place pour mettre à mal une attaque par mesure de consommation.

Références bibliographiques (ÉTAPE 1)

[1] NEWAE TECHNOLOGY INC. : ChipWhisperer® documentation and Side Channel Attack wiki *: https://wiki.newae.com/*

[2] ERIC BRIER, CHRISTOPHE CLAVIER, AND FRANCIS OLIVIER : Correlation Power Analysis with a Leakage Model *: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 3156, pp. 16–29, 2004.*

[3] NICOLAS T. COURTOIS : All About Side Channel Attacks *: University College London, Applied Crypto COMPGA12, 2006-2013*

[4] STEFAN MANGARD, ELISABETH OSWALD AND THOMAS POPP : Power Analysis Attacks Revealing the Secrets of Smart Cards *: Editions Springer (2007), ISBN: 978-0-387-38162-6*

[5] NIST : Advanced Encryption Standard (AES) *: Federal Information Processing Standards Publication 197 November 26, 2001*

DOT

[1] *: Novembre 2021 : Rencontre avec un ingénieur spécialisé dans les attaques par canaux auxilliaires qui m'a amené à lire la référence [4]*

[2] *: Mars 2022 : Mise en place d'une preuve de concept infructueuse sur RSA (matériel inadapté)*

[3] *: Mars 2022 : Mise en place d'une preuve de concept infructueuse sur RSA (matériel inadapté)*

[4] *: Décembre 2022 : Mise en place d'un filtrage Savitzky–Golay et premièrs résultats qualitatifs*

[5] *: Janvier 2023 : Mise en place d'un algorithme par fenêtre glissante, résultats quantitatifs*

[6] *: Mars 2023 : Mise en place d'une nouvelle attaque par corrélation sur AES, principe de base et corrélation de Pearson selon [2] et [5]*

[7] *: Avril-Mai 2023 : Réussite d'une attaque sur AES sur un jeu de données de test d'exemple*

[8] *: Juin 2023 : Extension et optimisation du code pour adapter l'attaque à un cas réel et des mesures expérimentales*